ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

Лицензия Microsoft Windows Server Std 2022 RUS, 16 ядер, OEM с носителем

P73-08337-LC

Описание

Microsoft Windows Server Standard 2022 – серверная операционная система, построенная на Windows Server 2022. Решение предлагает новый уровень безопасности и инноваций для приложений и инфраструктуры компаний. Многочисленные нововведения внедрены в гибридную, безопасную, прикладную платформу и инфраструктуру с гиперконвертированием. ОС Microsoft Windows Server Standard 2022 предназначена для сред с низкой плотностью и не ориентирована на виртуализированные системы.

Безопасность
Новые возможности обеспечения безопасности в Windows Server 2022 сочетают в себе другие возможности обеспечения безопасности Windows Server в разных областях. Это обеспечивает надежную защиту от дополнительных угроз. Расширенная многоуровневая защита в Windows Server 2022 предоставляет комплексную защиту, которая в настоящее время необходима серверам.
Сервер с защищенным ядром
Сертифицированное серверное оборудование с защищенным ядром от партнера OEM обеспечивает дополнительную защиту от изощренных атак. Это помогает обеспечить повышенную надежность при работе с критически важными данными в некоторых отраслях, где важна конфиденциальность данных. Сервер с защищенным ядром использует возможности оборудования, встроенного ПО и драйверов для включения расширенных функций безопасности Windows Server. Многие из этих функций доступны на компьютерах Windows с защищенным ядром, а теперь также доступны при использовании серверного оборудования с защищенным ядром и Windows Server 2022.
Корень доверия оборудования
Защищенные микросхемы криптопроцессоров доверенного платформенного модуля 2.0 (TPM 2.0) обеспечивают безопасное аппаратное хранилище конфиденциальных криптографических ключей и данных, включая результаты измерений целостности системы. TPM 2.0 позволяет убедиться, что сервер запущен с допустимым кодом и может быть доверенным при последующем выполнении кода. Эта возможность называется корнем доверия оборудования и используется такими функциями, как шифрование диска BitLocker.
Защита встроенного ПО
Встроенное ПО работает с высокими привилегиями и часто невидимо для традиционных антивирусных решений, что привело к увеличению количества атак с соответствующим направлением. Серверные процессоры с защищенным ядром поддерживают возможности измерения и проверки процессов загрузки с помощью технологии DRTM и изоляции доступа драйверов к памяти с помощью технологии защиты DMA.
Безопасность на базе виртуализации (VBS)
Серверы с защищенным ядром поддерживают технологии защиты на основе виртуализации (VBS) и обеспечения целостности кода на основе гипервизора (HVCI). VBS использует функции аппаратной виртуализации для создания и изоляции безопасной области памяти от обычной операционной системы, защищая от целого класса уязвимостей, используемых в атаках майнинга криптовалюты. VBS также позволяет применять Credential Guard, чтобы учетные данные и секреты пользователя хранились в виртуальном контейнере, к которому операционная система не может получить доступ напрямую.
HVCI использует VBS для значительного усиления соблюдения политики целостности кода, включая целостность режима ядра, которая проверяет все драйверы режима ядра и двоичные файлы в виртуализированной среде перед их запуском, предотвращая загрузку неподписанных драйверов или системных файлов в системную память.
Безопасное подключение
Транспортировка: протоколы HTTPS и TLS 1.3 по умолчанию включены в Windows Server 2022
Безопасные подключения являются основой современных взаимосвязанных систем. Протокол TLS 1.3 — это последняя версия наиболее популярной процедуры обеспечения безопасности в Интернете, которая позволяет шифровать данные для обеспечения безопасного канала связи между двумя конечными точками. Протоколы

ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

HTTPS и TLS 1.3 теперь включены по умолчанию в Windows Server 2022. Они защищают данные клиентов, подключающихся к серверу. Это позволяет отказаться от устаревших алгоритмов шифрования и повысить уровень безопасности по сравнению с более старыми версиями. Кроме того, эти протоколы предоставляют возможность шифровать максимально возможное количество подтверждений.

Безопасный клиент DNS: шифрование запросов разрешения DNS-имени с помощью клиента DNS по протоколу HTTPS

Клиент DNS в Windows Server 2022 теперь поддерживает использование клиента DNS по протоколу HTTPS (DoH), который шифрует запросы DNS по протоколу HTTPS. Это позволяет сохранять ваш трафик максимально закрытым, предотвращая перехват и изменение данных DNS.

Протокол SMB: шифрование SMB AES-256 для обеспечения максимальной безопасности

Windows Server теперь поддерживает наборы шифрования AES-256-GCM и AES-256-CCM для шифрования SMB. Windows будет автоматически согласовывать этот более сложный метод шифрования при подключении к другому компьютеру, который его поддерживает. Кроме того, этот метод можно сделать обязательным с использованием в групповой политике. Windows Server по-прежнему поддерживает шифрование AES-128 для обеспечения совместимости нижнего уровня. Процесс AES-128-HMAC теперь также повышает производительность подписывания.

Протокол SMB: элементы управления шифрованием SMB в направлении с востока на запад для обмена данными между внутренними кластерами

Отказоустойчивые кластеры Windows Server теперь поддерживают гибкий контроль над шифрованием и подписыванием обмена данными внутри узлов для общих томов кластера (CSV) и уровня шины хранилища (SBL). Это означает, что при использовании Локальных дисковых пространств и вы можете шифровать и подписывать обмен данными в направлении с востока на запад в самом кластере для повышения безопасности.

Шифрование SMB Direct и RDMA

SMB Direct и RDMA предоставляют высокую пропускную способность, сетевую структуру с низкой задержкой для рабочих нагрузок, таких как Локальные дисковые пространства, реплика хранилища, Hyper-V, масштабируемый файловый сервер и SQL Server. Функция SMB Direct в Windows Server 2022 теперь поддерживает шифрование. Раньше при включении шифрования SMB функция прямого размещения данных отключалась. Это было сделано намеренно. Однако это серьезно влияло на производительность. Теперь шифрование данных выполняется до размещения, благодаря чему происходит относительно небольшое снижение производительности при добавлении конфиденциальности пакетов, защищаемых с помощью AES-128 и AES-256.

SMB по QUIC

Использование протокола SMB по QUIC позволяет обновить SMB 3.1.1 в Windows Server 2022 Datacenter: Azure Edition и поддерживаемые клиенты Windows для использования протокола QUIC вместо TCP. Используя протокол SMB по QUIC вместе с TLS 1.3, пользователи и приложения могут безопасно и надежно получать доступ к данным из пограничных файловых серверов, работающих в Azure. Пользователям мобильных устройств и удаленным сотрудникам больше не нужен VPN для доступа к своим файловым серверам по протоколу SMB при использовании Windows.

Гибридные возможности Azure

Вы можете повысить эффективность и гибкость благодаря встроенным гибридным возможностям в Windows Server 2022, которые позволяют расширять центры обработки данных в Azure гораздо удобнее.

Серверы Windows с поддержкой Azure Arc

Серверы с поддержкой Azure Arc с Windows Server 2022 переносят локальные и многооблачные серверы Windows в Azure с помощью Azure Arc. Этот процесс управления предназначен для согласованного управления собственными виртуальными машинами Azure. Если компьютер с гибридной рабочей ролью, не относящийся к Azure, подключен к Azure, он становится подключенным компьютером и рассматривается как ресурс в Azure.